PENGGUNAAN SINGLE SIGN ON (SSO) PADA JARINGAN INTERNET BADAN PENGKAJIAN DAN PENERAPAN TEKNOLOGI (BPPT)

Johan Muliadi Kerta; Panji Adiprabowo; Eva Kusmiyati; Sylvia Astri Wulandari Rahardjo

Information Systems Department, School of Information Systems, Binus University
Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
johanmk@binus.ac.id

ABSTRACT

Using various applications needs more than one authentication or user and password to login. Users in BPPT found this problem on their network application. Implementation of Single Sign On can help users to use only one authentication for many applications. Therefore a research is conducted to design and implement Single Sign On system that simplify and facilitate the user's email account to access application. Data are collected from literature study, system observation, and interviews while the design uses Network Development Life Cycle (NDLC) method. The research results in a Single Sign On system that utilizez Lightweight Directory Access Protocol (LDAP). In addition, Remote Authentication Dial-In User Service (RADIUS) is managed in accordance with the needs of the institution. Single Sign On system designed runs well and is able to provide conveniences for the user to use the services of existing applications, as it provides a standard email address to the user's identity. It also helps administrators to perform control of users trying to login.

Keywords: *authentication, Single Sign On, LDAP, RADIUS*

ABSTRAK

Aplikasi yang banyak digunakan di BPTT mengakibatkan penggunaan otentikasi (user dan password) yang beragam untuk login. Masalah ini dihadapi oleh user di BPTT untuk mengakses aplikasi-aplikasi tersebut. Penerapan Single Sign On (SSO) dapat membantu user menggunakan hanya satu user dan password untuk beberapa aplikasi. Maka dari itu penelitian ini dilakukan untuk merancang dan mengimplementasikan sistem SSO untuk menyederhanakan akun email dan memudahkan user dalam mengakses layanan aplikasi. Pengumpulan data meliputi studi kepustakaan, observasi sistem, dan wawancara. sedangkan perancangan menggunakan metode Network Development Life Cycle (NDLC). Dari penelitian ini dihasilkan sistem Single Sign On yang menggunakan protokol Lightweight Directory Access Protocol (LDAP). Selain itu, Remote Authentication Dial-In User Service (RADIUS) telah sesuai dengan kebutuhan perusahaan. Sistem SSO yang dirancang berjalan dengan baik dan dapat memberikan kemudahan bagi user untuk menggunakan layanan aplikasi, serta memberikan identitas email bagi user yang terstandarisasi dan membantu administrator melakukan kontrol terhadap user yang mencoba login.

Kata kunci*: otentikasi, Single Sign On, LDAP, RADIUS*

PENDAHULUAN

Jaringan komputer merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan (interkoneksi) dalam melaksanakan tugas-tugas komputasi suatu organisasi (Tanenbaum, 2003, p.1). Badan Pengkajian dan Penerapan Teknologi (BPPT) merupakan salah satu instansi pemerintah yang memiliki sekitar tiga ribu orang pegawai. BPPT mempunyai banyak aplikasi lokal yang pengaksesannya memerlukan *authentication*. Hal ini menjadi masalah dimana *user-user* tersebut harus menghapalkan ID *user* (*user*name dan *password*) yang disimpan dalam *database* masing-masing aplikasi. Sedangkan untuk mengakses internet karyawan hanya perlu memasukkan alamat proxy dan port yang diizinkan. Saat ini, tidak ada pembatasan hak untuk mengakses internet sehingga setiap orang yang mengetahui alamat proxy dan port dapat menggunakan internet dengan bebas.

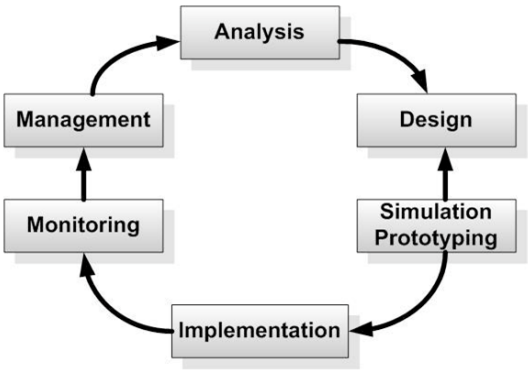
Dilihat dari pendekatan tersebut, BPPT memerlukan sebuah sistem *Single Sign On* (SSO) yang dapat menyederhanakan jumlah akun dan mendukung protokol AAA (Authentication, Authorization, Accounting). Operasi AAA dimulai dengan proses *authentication* yaitu proses yang mengesahkan identitas *user*. *User* yang telah teridentifikasi melalui *user* ID belum tentu adalah pemilik *user* ID yang sesungguhnya. Maka dari itu, dibutuhkan proses *authentication* untuk memastikannya. Sistem akan meminta *user* untuk memberikan bukti supaya identitas *user* dapat terbukti. Bukti yang diberikan oleh *user* dalam proses *authentication* biasa disebut *credential*. *Credential* biasanya berbentuk *password*, angka PIN, dan merupakan rahasia yang hanya diketahui oleh *user* dan sistem. Dengan kata lain, *authentication* adalah proses untuk memastikan identitas *user* yang sudah teridentifikasi menggunakan bukti yang sudah disediakan oleh *user* (Nakhjiri & Nakhjiri, 2005, p.1). Kemudian proses otorisasi ditunjukkan dengan pemberian hak akses kepada pengguna. Untuk akuntansi, sistem mencatat kegiatan/log request dari client ke sistem. Untuk menunjang sistem SSO ini, diperlukan sebuah direktori berupa *Lightweight Directory Access Protocol* (LDAP) dan protokol *Remote Authentication Dial In User* (RADIUS). RADIUS adalah protokol standar industri yang dijelaskan dalam RFC 2865, "Remote Authentication Dial-In *User* Service (RADIUS)", dan RFC 2886, "RADIUS Accounting". RADIUS digunakan untuk menyediakan layanan *authentication*, otorisasi, dan akuntasi atau auditing. Client RADIUS mengirimkan data *user* dan informasi parameter koneksi dalam bentuk pesan RADIUS ke *server* RADIUS. *Server* RADIUS meng-*authentication* dan meng-otorisasi permintaan client RADIUS, dan mengirimkan kembali sebuah respon dari pesan RADIUS. Client RADIUS juga mengirimkan pesan akuntasi RADIUS ke *server* RADIUS (Hassel, 2002).

METODE

Metode yang digunakan dalam penulisan skripsi ini meliputi dua bagian pokok. Pertama adalah pengumpulan data menggunakan: (1) observasi sistem, yaitu melihat dan mengamati secara langsung sistem jaringan yang sedang berjalan di gedung BPPT; (2) wawancara kepada pihak terkait untuk mengetahui sistem yang sedang berjalan dan sistem baru yang diinginkan oleh BPPT; (3) studi kepustakaan, yaitu mengumpulkan data-data yang telah terdokumentasi dari sistem yang sedang berjalan.

Bagian kedua yaitu perancangan dan pengembangan sistem yang sedang berjalan menggunakan *Network Development Life Cycle* (NDLC) yang terdiri dari enam tahap, yaitu *analysis, design, simulation prototyping, implementation, monitoring* dan *management* (Gambar 1). Siklus ini bersifat terus-menerus karena merupakan tuntutan dari sebuah jaringan yang berada pada kondisi yang terus-menerus berubah karena perubahan dalam bisnis, aplikasi, atau kebutuhan data, sehingga desain

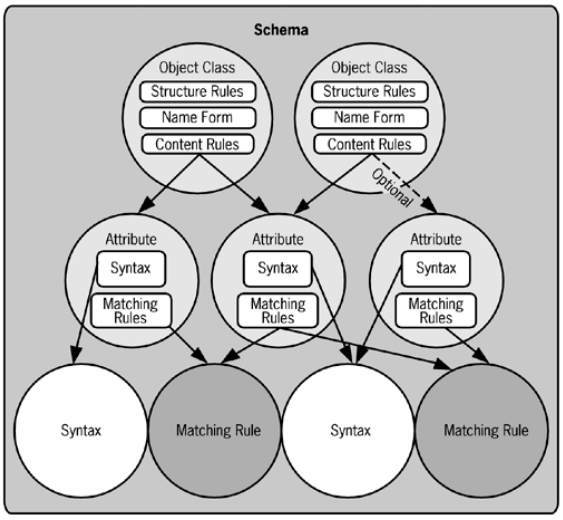
jaringan sendiri harus bersifat dinamis supaya bisa mendukung perubahan-perubahan kebutuhan ini. (Goldman & Rawles, 2004, p.378).



Gambar 1. Network Development Lifecycle (sumber: Goldman & Rawles, 2004, p.378).

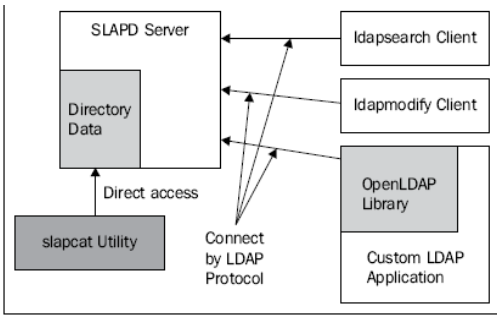
HASIL DAN PEMBAHASAN

Penggunaan Lightweight *Directory* Access Protocol (LDAP) adalah untuk menyeragamkan metode *user* access. Disebut Lightweigth karena sifatnya yang relatif tidak memberatkan. LDAP menggunakan *low level message* yang dipetakan secara langsung ke dalam *layer* TCP (biasanya port 389) dari stack protokol TCP/IP. Berbeda dengan X.500, karena X.500 adalah protokol *layer* aplikasi, ini membawa lebih banyak beban disebabkan header jaringan dibungkus di sekeliling paket di setiap *layer* sebelum akhirnya ditransmisikan ke jaringan. (Carter, 2003). Skema LDAP dapat dilihat pada Gambar 2 berikut.



Gambar 1. Skema LDAP (sumber: Arkills, 2003).

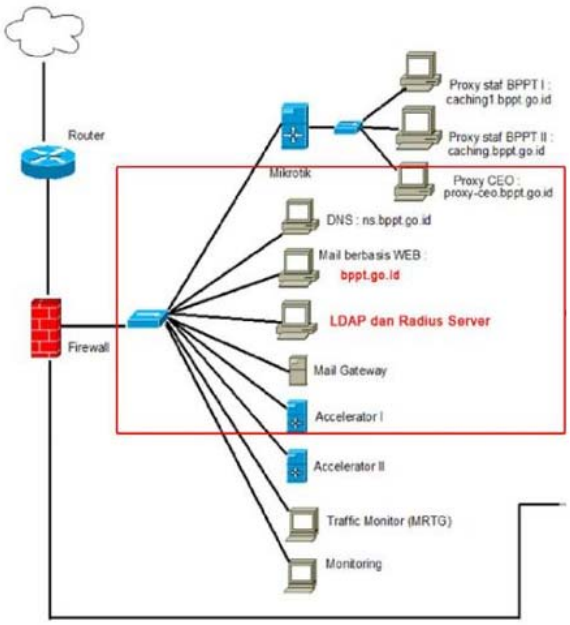
Application Programming Interfaces (APIs) disediakan untuk mengizinkan para pengembang perangkat lunak menulis aplikasi LDAP mereka sendiri tanpa menulis ulang kode dasar LDAP. Jika API yang disediakan untuk OpenLDAP ditulis dalam bahasa C, proyek OpenLDAP juga menyediakan dua Java API (Butcher, 2007, p21).



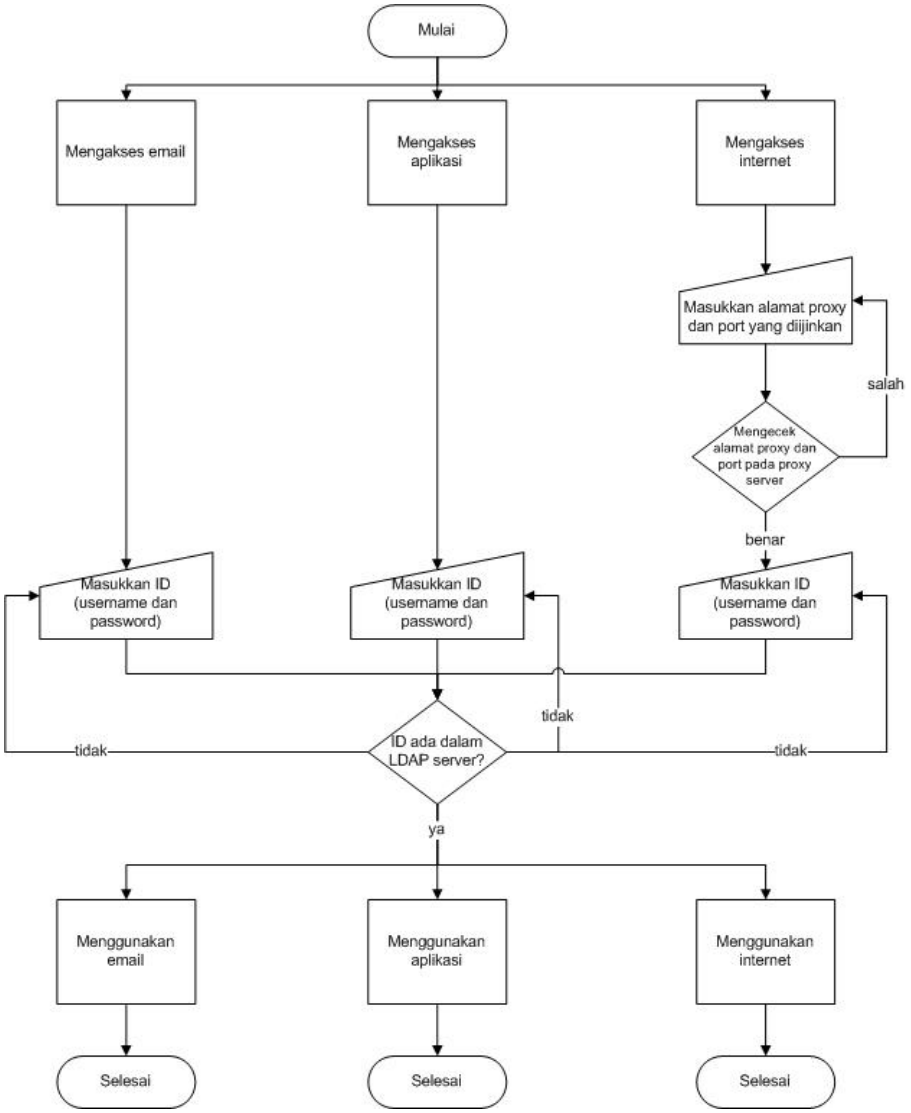
Gambar 2. Diagram komponen OpenLDAP (sumber: Butcher, 2007).

Model penamaan mendefinisikan bagaimana *entry* dan data di *Directory* Information Tree (DIT) dirujuk secara unik. Setiap *entry* memiliki sebuah atribut yang unik di antara semua saudaranya dari satu *single parent*. Atribut yang unik ini disebut relative *distinguised name* (RDN). Setiap *entry* apapun di dalam direktori bisa diidentifikasi secara unik dengan mengikuti RDN dari semua *entry* di path dari *node* yang diinginkan sampai ke *root* dari pohon. *String* dibuat dengan mengkombinasikan RDN untuk membentuk sebuah nama unik yang disebut *node's distinguished name* (DN) (Carter, 2003). *Directory* secara umum adalah sebuah daftar dari informasi tentang obyek-obyek yang tersusun dalam urutan tertentu dan memberikan detail dari setiap obyek dan bertujuan untuk menyimpan informasi statis, seperti alamat, nomor telepon, dan tidak cocok untuk menyimpan informasi yang berubah secara cepat. *Directory* dapat dioptimasikan secara ekonomis untuk menyediakan banyak aplikasi dengan akses cepat menuju *Directory* data dalam lingkungan distribusi yang besar (Tuttle, 2004, p. 5).

Rancangan topologi jaringan dilakukan dengan melakukan penambahan *server* LDAP dan RADIUS seperti yang ada pada Gambar 4. Sedangkan perancangan dan cara kerja sistem secara keseluruhan dapat dilihat pada Gambar 5. Pada akhirnya aplikasi administrasi antara administrator dan *user* dapat digambarkan dengan interaksi yang terjadi pada *use case* di Gambar 6.



Gambar 3. Gambar Rancangan Jaringan dengan LDAP dan E-Mail



Gambar 5. Flowchart cara kerja sistem.

Evaluasi Sistem

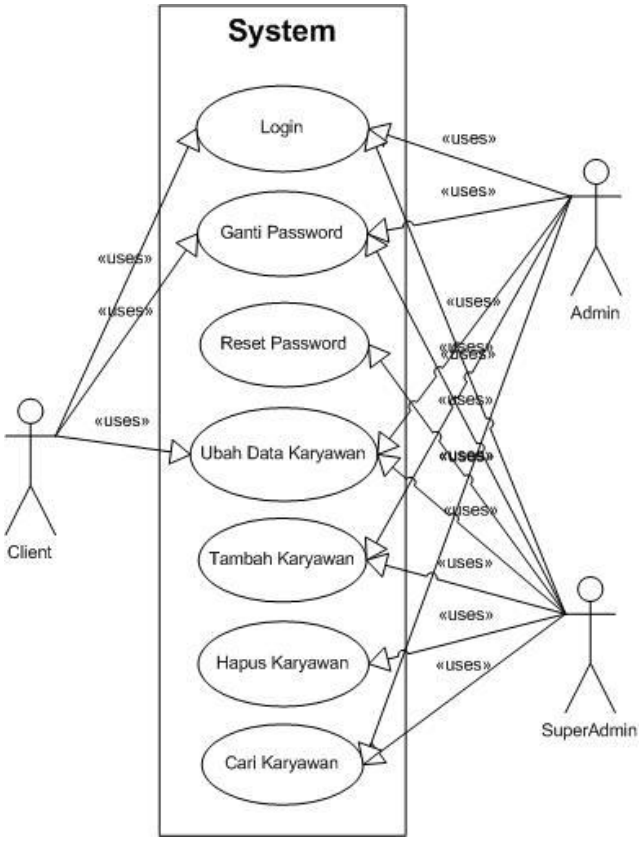
Evaluasi dilakukan untuk menilai kerja sistem secara keseluruhan dengan melakukan pengumpulan data berupa kuesioner sebagai berikut:

Pertanyaan 1: Setelah diterapkannya sistem SSO ini, seberapa sering Anda salah memasukkan *password*?. Sebanyak 27% *user* menyatakan tidak pernah lagi salah memasukkan *password* mereka saat *login*. Sisanya, 73% *user* menyatakan jarang melakukan kesalahan saat memasukkan *password* untuk *login*. Dengan hasil tersebut dapat dikatakan bahwa *user* lebih mudah mengingat *user* dan *password*nya karena penggunaan *user* dan *password* yang sama untuk aplikasi yang digunakan.

Pertanyaan 2: Bagaimanakah layanan email yang baru (Zimbra), khususnya untuk tampilan dan fitur?. Sebanyak 73% *user* menyatakan tampilan dan fitur email Zimbra baik. Sedangkan 18% *user* lainnya menyatakan bahwa tampilan dan fitur email Zimbra sangat baik. Sebanyak 9% menyatakan bahwa tampilan dan fitur Zimbra cukup baik. Penggunaan *user interface* email yang baru

meningkatkan penggunaan media email untuk berkomunikasi melalui internet. Tambahan lagi, penggunaan domain yang seragam memudahkan *user* untuk mengingat dan memiliki identitas yang sama.

Pertanyaan 3: Bagaimana kemudahan mengakses internet di BPPT dengan sistem yang baru ini?. Semua *user* atau 100% *user* menyatakan tingkat kemudahan untuk mengakses internet di BPPT adalah mudah untuk digunakan. Penggunaan LDAP dalam *Single Sign On* ini tidak mengubah cara kerja sistem *authentication* yang selama ini digunakan sehingga *user* merasakan kemudahan dan nilai tambah dari penggunaan sistem ini. Pertanyaan 4: Bagaimana tingkat kepuasan Anda terhadap sistem secara keseluruhan?. 82% *user* puas dengan adanya sistem *Single Sign On* ini. Lalu, sebanyak 9% *user* menyatakan sangat puas dengan sistem *Single Sign On* yang telah diterapkan. Dan sebanyak 9%, menyatakan cukup puas dengan adanya sistem *Single Sign On* ini.



Gambar 6. Use Case untuk *Client* dan *Administrators*

PENUTUP

Simpulan yang didapat berdasarkan hasil analisis dan perancangan, pengujian, implementasi, evaluasi, adalah: (1) Terciptanya sistem *Single Sign On* yang menyediakan kenyamanan bagi *user* dalam hal integrasi *username* dan *password* untuk setiap layanan; (2) Penyederhanaan domain email BPPT membuat *user* mempunyai identitas tunggal dalam pengiriman pesan; (3) Penggunaan LDAP membuat *database user* menjadi terpusat sehingga memudahkan manajemen akun *user*; (4) Hanya *user* yang *authenticated* yang dapat mengakses layanan-layanan yang ada karena adanya keharusan untuk melakukan *login*; (5) adanya *data log* RADIUS membantu administrator melihat *list user* yang

mencoba untuk *login*. Hal tersebut dapat menjadi salah satu sumber untuk mengetahui adanya pola yang mencurigakan, misalnya ada *user* ataupun orang lain yang mencoba *login* berkali-kali dengan menggunakan ID *user* lain; (6) struktur identitas yang lebih baik berhasil dibuat.

Sedangkan saran yang diajukan terkait dengan penggunaan sistem ini adalah: (1) memperluas penerapan system *Single Sign On* sehingga dapat mencakup semua jenis aplikasi, seperti aplikasi *desktop* yang digunakan saat ini; (2) meningkatkan fungsi *accountability* dari RADIUS dengan menambahkan keamanan misalnya menggunakan *firewall* sebelum RADIUS; (3) mengembangkan sistem sinkronisasi antara LDAP dengan mail *server* (Zimbra) untuk memudahkan kerja administrator; (4) membuat sistem *back-up* secara keseluruhan data baik data email, *database user* maupun data pada aplikasi-aplikasi yang digunakan.

DAFTAR PUSTAKA

Arkills, Brian. (2003). *LDAP Directories Explained: An Introduction and Analysis*. Boston: Addison-Wesley.

Butcher, Matt. (2007). *Mastering OpenLDAP*. Birmingham: Packt Publishing.

Carter, Gerard. (2003). *LDAP System Administration.* California: O'Reilly.

Goldman, James E., & Rawles, Phillip T. (2004). *Applied Data Communications A Business-Oriented Approach* (4th ed.). New Jersey: John Wiley & Sons.

Hassel, Jonathan. (2002). *RADIUS*. California: O'Reilly.

Nakhjiri, Madjid & Nakhjiri, Mahsa. (2005). *AAA and Network Security for Mobile Access*. West Sussex: John Wiley & Sons.

Tanenbaum, Andrew S. (2003). *Computer Networks* (4th ed.). Boston: Pearson Education.

Tuttle, S., Ehlenberger, A., Gorthi, R., Leiserson, J., Macbeth, R. et al. (2004). *Understanding LDAP Design and Implementation.* New York: International Business Machines Corporation.